REMARKS

Claims 1-25 were withdrawn from consideration. In the Previous Office Action Response, Applicants argued that Brewer does not teach or suggest any security control indicator that is used to determine if the frame is encrypted and authenticated. Claim 26 has been amended to correct informalities. The Examiner is now rejecting the claims under new grounds. Claims 26-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

Hawe describes a cryptographic preamble. "More specifically, the offset field included in the cryptographic preamble indicates a number of data elements to skip to the start of the material to be cryptographically processed. In the method of the invention, this offset is used to skip over header information in the packet, which may vary in length and content depending on the protocol under which the packet was generated. The cryptographic preamble further includes a mode field indicating the type of cryptographic processing to be performed, and the step of performing the cryptographic processing includes conditioning the cryptographic processor to perform the type of processing requested in the mode field. The available modes include encrypting for outbound transmission, encrypting or decrypting for loopback to the node processor, encrypting a cipher key for loopback to the node processor, and computing an integrity check value for loopback to the node processor." (column 3, lines 36-64)

Hagerman describes "A Fibre Channel storage area network utilizes frames having time-of-transmission and authentication-code fields. These fields are in addition to the normal fields of Fibre Channel frame headers, and may be implemented as a higher-level protocol encapsulated in the data portion of each frame or may be embedded in an enhanced frame header. The time-of-transmission field is derived from a real-time clock on each node. The real-time clock is incremented quickly enough that no two frames transmitted within a reasonable time of each other will have the same time-of-transmission field contents." (column 3, lines 23-33).

The Examiner relies on Hawe to describe "receiving a frame at a first network entity from the second network entity in a fibre channel network" and "identifying a security control indicator in the frame from the second network entity, wherein the security control indicator is used to determine if the frame is encrypted and authenticated." The Examiner argues that Hawe

has a cryptographic preamble and an offset field used to determine if the frame is encrypted. However, the cryptographic preamble and offset field are not transmitted in any frame as recited in the independent claims. The independent claims explicitly recite receiving a frame at a first network entity from the second network entity and identifying a security control indicator in the frame from the second network entity. Hawe does not teach or suggest any security control indicator that can be transmitted to a first network entity from a second network entity. Even if the cryptographic preamble and the offset field are assumed to be the security control indicator, Hawe does not transmit the cryptographic preamble or the offset field.

Hawe states that "The invention comprises the steps of appending a cryptographic preamble to the beginning of an information packet for which cryptographic processing is needed; passing the information packet to a cryptographic processor; detecting, in the cryptographic processor, that cryptographic processing is needed; analyzing the cryptographic preamble to determine the location in the packet of material to be cryptographically processed, and the type of cryptographic processing to be performed; performing the requested cryptographic processing; and stripping the cryptographic preamble from the packet if the packet is to be transmitted onto the network, to preserve compatibility with existing packet formats transmitted over the network." (column 3, lines 15-23) Hawe explicitly requires "stripping the cryptographic preamble from the packet if the packet is to be transmitted onto the network, to preserve compatibility with existing packet formats transmitted over the network." (column 3, lines 22-23) Hawe not only does not teach or suggest all of the elements of the independent claims, Hawe actually teaches away from the techniques and mechanisms of the present invention.

By contrast, the techniques and mechanisms of the present invention recognize that having a security control indicator allows processing under a standard protocol that does not support encryption. For example, "Figure 10 is a process flow diagram showing a network node in a fibre channel fabric receiving a frame. At 1001, the frame is received. At 1003, it is determined if the frame is secured. Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security. A frame that supports encryption and authentication is herein referred to as a secured frame. A frame that supports only authentication

is herein referred to as an authentication secured frame. A frame that supports only encryption is herein referred to as an encryption secured frame."

That is a conventional protocol such as a conventional fibre channel protocol can be used. "If the frame is not secured, processing proceeds using a conventional fibre channel protocol. If the frame is secured, an identifier such as a security parameters identifier SPI is referenced against a security database such as a security association database at 1005. Key information and algorithm information are extracted from the entry containing the identifier or security parameters index associated with the received frame." According to various embodiments, the encryption method is obtained from the security association database. Consequently, Brewer actually indicates that it does not have a security association database because the encryption methodology is included in the encryption methodology field in the header. The network interface card (NIC) of Brewer can then quickly perform decryption using information from the header without having the overhead of accessing any database to determine methodology. This combined with the fact that Brewer does not explicitly describe any security association database suggests that Brewer does not use any security association database as recited in the independent claims.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/G. Audrey Kwan/
G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100